REMARKS/ARGUMENTS

Claims 1- 29 and new claims 30 and 31 are pending in the application. Reconsideration is requested in view of the above amendments and the following remarks.

Applicant acknowledges that the replacement drawing has been accepted.

Applicant also notes that the section 101 rejection has been traversed.

The Examiner has withdrawn the prior rejections in view of new rejections which are set forth in the final office action.[1] Applicant notes the additional references cited, and respectfully traverses these rejections.

New claims 30 and 31 have been added to round out coverage for the invention and depends from claim 1. New claim 30 recites initiating a client process from a computer and wherein providing a hash code table of a client comprises providing a hash code table for the computer from which the client process was initiated. New claim 31 further distinguishes the present invention by reciting that the client state code is transmitted along with authentication. Allowance of new claims 30 and 31 is respectfully solicited.

Applicant's remarks are set forth below.

[1] Though there appears to be a 102 rejection over Nachenberg ,there are no reasons presented, and, in view of the Examiner's statement that the prior rejections are moot, Applicant deems the 102 paragraph in the Office Action to appear there in error. If there is a 102 rejection, however, Applicant respectfully requests that the date be reset.

1. The Section 103 Rejection of the Claims as Being Obvious Over Liu, Nachenberg and Small Should be Withdrawn.

Claims 1, 8, 11, 13, 16-19, 21-23, 25, 28 and 29 stand rejected under 35 U.S.C. 103(a) as being obvious over Liu (US 7,096493) in view of Nachenberg (US 6,021,510) in further view of Small (US 6,145,012). This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection are hereby respectfully requested.

The Examiner considers that Liu discloses providing a hash code table of a client, said hash code table being provided for storing a plurality of files, citing to Liu at col. 3 line 60 through col. 4 line 8); and that Liu discloses providing a client state code of a client and comparing the client state code to the hash code table (citing to Liu at col. 4 lines 25-29). The Office Actions further considers Liu to disclose a secure hash code table that includes the hash codes for files on computers within the network that are to be secured (col. 3, line 60 through col. 4 line 8). The Office Action considers Liu to provide a method of transmitting across a network from clients located in the network client state code; and providing a server within the network assigned to recognize the client state code transmission (col. 4 lines 25-51); and further claims that Liu discloses a server that maintains a listing of files comprising a hash code table of clients.

The Examiner acknowledges that Liu fails to disclose features of the Applicant's claimed invention, including generating an alert mechanism when a deviation threshold is reached based on a deviation between said hash code table values for said client and said client state code, and that the server maintains a baseline for a client.

The Examiner attempts to fill these deficiencies with the additional references of Nachenberg (alleging reference to an alert at col. 4 lines 54-64) and Small (alleging reference to a server maintaining a baseline for a client at col. 4 lines 19-47). The Office Action considers the motivation to modify Liu would be found at Nachenberg col. 4 lines 54-64, and Small at col. 2 lines 14-20).

This rejection is respectfully but strenuously traversed. Applicant's invention is not taught, suggested or disclosed by the cited references. Applicant's invention is directed to providing secure systems on a network. The systems on the network may be monitored and controlled. Applicant's invention employs and claims utilization of a client state code for systems on the network. (See Applicant's published specification at [0014]) It is the client state code, corresponding to the system or client on the network which may be used to provide the baseline configuration for that client, or other clients as well. The Applicant's invention facilitates a secure network.

Liu, on the other hand, relates to files coming from public distribution (col. 3, lines 55-59, and see col. 4, lines 29-31), as opposed to files of systems on a secure network. Liu discusses file distribution from a client perspective where a client attempts to authenticate a file, not maintain a client state code or baseline configuration. One reading Liu's disclosure would not arrive at the Applicant's claimed invention. Applicant's invention relates to methods, apparatus and articles of manufacture for securing, maintaining, monitoring and controlling systems and networks. A secure hash code table is generated or derived and provides a baseline for the network and the

systems on the network. (See Applicant's published specification at par. [0013].) Applicant accomplishes this by utilizing a comparison cycle, wherein one or more systems or components on the network transmits a client state code. The client state code is compared to the secure hash code table value. If the client state code does not deviate from the secure hash code table value, or, alternately, if the deviation is within certain acceptable ranges (e.g., where a modal hash is derived) then the baseline may be considered to represent the acceptable client state and no further action needs to be taken. If deviation is uncovered (in any manner or by an amount deemed unacceptable) an alerting mechanism is triggered.

There is not a disclosure of Liu of providing an acceptable client state. Rather, the client state is disregarded in Liu, as Liu attempts to provide a method for authenticating files from a public source for a client to load. Liu discloses and relates to a method for authenticating a file which is to alter the client state, and would appear to teach or suggest doing so without regard to maintaining the integrity of the client state. Rather, the file is authenticated so the client, once having authenticated the file may actually change the client state.

The Office Action considers that Liu discloses a server maintaining a listing of files for clients. That is not a disclosure of the Applicant's invention, nor does Liu's alleged maintained listing provide the baseline configuration for clients. Liu is concerned with public files, not integrity of what is already on the client. Liu teaches and discloses doing the opposite of what the Applicant does. Public files that are authenticated for

addition to the client, as Liu appears to relate, would not maintain a client state, or baseline, in the manner disclosed and claimed by the Applicant.

Applicant's invention, in claim 1, specifically recites that the ***secure hash code table includes the hash codes for files on computers within the network that are to be secured***. This is not disclosed or taught in Liu. First, according to Applicant's invention, the hash code table is secure. Second, the secure hash code table includes hash codes for files on computers within the network that are to be secured. Computers on the network that are to be secured are represented by the secure hash code table. This is contrary to introduction of public files. Unlike the present invention, Liu's disclosure appears to relate to authenticating a file not on the secured computer on the secured network, but rather, a file from a public source.

The Office Action further refers to Fig. 1a of Liu for a disclosure that the server maintains a listing of files for clients, and that the listing of files comprises hash code table of clients. Again, Liu does not appear to provide the recited features of the presently claimed invention. Liu does not disclose providing a hash code table for the computer from which the client process was initiated (see Fig. 1b). (See e.g., new claim 30.) Rather, there is a file authentication, not securing a baseline configuration of a client. Liu illustrates the web server (102) apparently outside of the secured network where the client and server are located.

It does not appear that Liu discloses the hash code table of clients, let alone a hash code table of clients on a secure network. Liu does not appear to distinguish clients on

the basis of a baseline configuration. Rather, Liu appears to relate to files which a client may desire to install (e.g., disruption of baseline configuration). In other words, Liu cannot teach the Applicant's invention where Liu's very disclosure disregards baseline configuration maintenance of a client. Liu would teach away from the present invention.

Applicant's invention is further distinguishable over Liu. Transmission of system state data to a server is a featured step of the Applicant's claimed invention. Claim 1 also recites providing a client state code of a client. This feature and disclosure is not provided by Liu.

Further distinguishing Liu is Applicant's own specification which indicates that according to an alternate embodiment, the client state code is transmitted along with authentication. Liu discusses authentication, whereas, Applicant provides a client sate code (not disclosed or taught by Liu) and, in addition, may utilize authentication for the communication between the client and server. (See Applicant's specification at [0037]; and see new claim 31.) Liu does not utilize a secure network, but discusses publicly distributed files, which are to be authenticated.

For the above reasons, Applicant's invention is not taught, suggested or disclosed by Liu.

Even when the additional references are combined, the deficiencies of Liu, still do not result in the teaching or disclosure of the Applicant's invention. Nachenberg is cited for an alleged teaching of an alert. However, if one of ordinary skill in the art reads Liu, and applies an alert, the alert would not relate to whether the client baseline configuration

has been maintained or changed. Rather, the alert would be understood to merely relate to some public file being acceptable or not acceptable.

In addition, the further addition of Small, which is alleged to teach a server maintaining a baseline, does not result in the present invention. Small discusses that the server computer stores a baseline file, and that the client computer makes a local copy of the baseline file, modifies the baseline file and stores a copy of the modified file. (Col. 3, lines 37-41). Small discloses modification of the server file with the modification of the client file. That is contrary to the Applicant's baseline integrity method, where the integrity of clients on a secured network are to be maintained and controlled. Again, similar to the reasons why Nachenberg would not be combined with Liu, attempting to modify Liu with Small would not serve Liu's purpose and would be inconsistent. After all, Liu attempts to authenticate public files which a client is attempting to obtain. Small relates to updating a file in a first computer to match a copy in a second computer. According to Small, a baseline file is used to make up, with modified portions of the client file, the destination file. This is not the Applicant's present invention, and one of ordinary skill in the art would not have arrived at the present invention by making a modification of Liu with the Small teachings. Applicant's invention provides a secure hash code table that includes the hash codes for files on computers within the network that are to be secured. Neither Liu nor Small provides this feature.

For the above reasons, Applicant's present invention is not taught, suggested or disclosed by the cited references. Reconsideration and a withdrawal of the rejection is respectfully requested.

2. The 103(a) Rejection Over Modified Liu, Nachenberg, Small and Angelo Should be Withdrawn.

Claims 2, 3, 6 and 20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over "modified Liu", Nachenberg and Small as applied to claims 1 and 19, and further in view of Angelo (U.S. 5,944,821). This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection are hereby respectfully requested.

The rejection in the Office Action relies on the Liu, Nachenberg and Small disclosures, discussed above. However, the rejection acknowledges that the cited references fail to disclose the hash code table being a secure hash code table. Angelo is relied on, therefore, for an alleged teaching of the use of a secure hash table (citing to col. 4, lines 27-40) with the contention that it would have been considered obvious to make a hash table of "modified Liu", Nachenberg and Small a secure hash table.

Applicant's invention as recited in claims 2, 3, 6 and 20 is not obvious in view of the cited references. First, for the same reasons set forth above as to why the Applicant's invention should be patentable Liu, Nachenberg and Small, even in view of the further combination of Angelo, the present invention is still not disclosed or suggested. Second, one of ordinary skill in the art looking to the cited references of Liu, Nachenberg and Small would not have been led to provide a secure hash table. One reason is that Applicant desires to consider a secure client state code, whereas Nachenberg seeks accelerating antivirus program speed by apparently attempting to prescan and store

certain prescan results. Another reason is that Liu would not be expected to be combinable with Angelo, nor would Angelo be looked at by one of ordinary skill in the art to be combined with the other references, namely, Nachenberg and Small. Angelo provides that the secure hash table is stored in protected memory and is only accessible in system management mode.

> In general, a secure hash table (or other type of integrity assessment code) is provided that contains a secure hash value for each program that the user wants to track. The hash table is stored in protected memory that can only be accessed when the computer system is in a system management mode. Execution of a secured application is then predicated on its current hash value matching a corresponding hash value in the secure hash table.
>
> (Angelo, col. 4, lines 30-37).
>
> More particularly, the invention improves upon the SAFESTART patent and similar concepts by allowing real-time secure access to and calculation of stored secure hash tables, stored hash values and hash algorithms for verifying the trustworthiness of applications prior to execution. In one embodiment of the invention, a secure hash value is generated for a piece of software when it is installed on the computer system. Once generated, the hash value for the newly-installed software is then stored in a secure hash table that contains hash entries for each protected application. A "secure hash value" in the preferred embodiment is 160 bits of data (20 bytes) that is essentially a mathematical representation of a file. If any bits in the file are changed, a different hash value will result.
>
> (Angelo, col. 4, lines 41-54).

One of ordinary skill in the art would not seek to modify Liu with Angelo. Liu is cited for its disclosure, which, at col. 4, lines 40-44, discloses that the Liu method begins with the client user portion and an identification of a file to authenticate. That would appear to be inconsistent with Angelo's disclosure of a hash table which is stored in protected memory that can only be accessed when the computer system is in a system management

mode. As discussed herein, Liu is understood to relate to a system for authenticating files which are publicly distributed.

For the above reasons, Applicant submits that Liu, Nachenberg Small and Angelo fail to disclose or suggest Applicant's present invention. Accordingly, reconsideration and a withdrawal of the rejection is respectfully requested.

3. The 103(a) Rejection of Claims 4, 5, 14, 15, and 26-27 Over Modified Liu, Nachenberg and Small (Alone or In Combination With Angelo) in Further View of Ward (US 6,526,411) Should be Withdrawn.

Claims 4, 5, 14, 15 and 26-27 stand rejected under 35 U.S.C. 103(a) as being unpatentable over modified Liu, Nachenberg and Small, alone or combination with Angelo, as applied to claims 3 and 25 above in view of Ward (US 6,526,411). This rejection is respectfully but strenuously traversed and reconsideration and withdrawal of the rejection is hereby respectfully requested.

The Examiner in the Office Action acknowledges that the cited references of Liu, Nachenberg and Small fail to disclose grouping (considered in the rejection to be compiled) the secured system data file and extracting the modal hash value. The Examiner, however, though acknowledging that these references fail to disclose these features of Applicant's claimed method, considers that it would have been obvious to take an additional reference, namely Ward, which is considered in the Office Action to teach grouping of files (citing to col. 3, lines 31-42), as well as the assertion that the motivation to do so would be to adapt the most common configuration among clients (citing to Ward at col. 1, lines 49-62) regarding extracting the modal hash value.

First, for the reasons set forth above distinguishing the Applicant's present invention over Liu, Nachenberg and Small and Angelo, the Applicant's invention should be patentable over these references even when the additional reference of Ward is proposed to be combined.

In addition, the substance of the rejection with the addition of Ward does not appear to come from the references themselves (e.g., Liu, Nachenberg, Small and Angelo), but rather, from Applicant's own disclosure, and should be withdrawn for that reason alone.

Moreover, Applicant's invention, however, does not simply relate to a most common value among any group, but rather to generating a secure hash code table using at least one compiled client hash value for a secure hash code table that includes the hash codes for files on computers within the network that are to be secured. It is the Applicant's disclosure and invention which seeks to secure clients within the network.

The passage actually relied on in Ward reads as follows, and does not provide the disclosure of Applicant's invention:

> The pairing sort algorithm as applied to at least one user profile begins with selecting a seed user profile, and processes the steps of comparing the seed user profile against all available profiles, ranking all compared profiles by similarity to the selected seed profile, clustering the most similar profiles with the seed profile, counting the frequency of all elements in the clustered profiles, building a hash profile of the most frequent items to represent each respective cluster, placing the respective hash profile in a hash table, removing the seed and clustered profiles from the profile list, identifying a next user profile, if available, as the seed user profile, and continuing the sequence until no profiles are available.
>
> (Ward col. 3, lines 31-42)

> It is therefore a principal object of the present invention to provide a dynamic playlist system and method for a dynamic playlist of digital items that automatically adds items to, or subtracts items from, the playlist, as the items become available.
>
> An object of the present invention is to provide the dynamic playlist system where the data items are music or video items.
>
> Another object of the present invention is to provide a dynamic playlist that dynamically adapts to usage patterns.
>
> Another object of the present invention is to provide a dynamic playlist that dynamically adapts to personal preferences.
>
> Another object of the present invention is to provide a dynamic playlist that is easy to use.
>
> (Ward col. 1, lines 49-62)

To the extent the rejection relies on Ward for an alleged teaching of "grouping files", what is actually referred to in Ward is taking a first and second item from a playlist, determining if both elements are in an elements table, and inserting whichever element is missing into the elements table.

For the above reasons, and for these additional reasons, the rejection of claims 4, 5, 14, 15 and 26-27 should be withdrawn.

4. The 103(a) Rejection of Claim 10 Over Liu, Nachenberg and Small and Adya Should be Withdrawn.

Claim 10 stands rejected under 35 U.S.C. 103(a) as being unpatentable over modified Liu, Nachenberg and Small, as applied to claim 1 above, and further in view of Adya et al. (US 20020188605). This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested.

The Examiner's rejection considers that modified Liu, Nachenberg and Small fail to disclose securing a client in lock down mode. The Examiner considers Adya et al. to teach this at paragraphs 144-146.

For the same reasons as set forth above, Applicant's invention is not obvious in view of the cited references even when the further combination with the Adya et al. reference is attempted. Reconsideration and a withdrawal of the rejection are hereby respectfully requested.

5. The 103(a) Rejection of Claims 12 and 24 Over Liu, Nachenberg and Small and Pascucci Should be Withdrawn.

Claims 12 and 24 stand rejected under 35 U.S.C. 103(a) as being unpatentable over modified Liu, Nachenberg and Small, as applied to claims 1 and 19 above, and further in view of Pascucci et al. (US 5,463,735). This rejection is respectfully but strenuously traversed and reconsideration and a withdrawal of the rejection is hereby respectfully requested.

The Examiner admits that modified Liu, Nachenberg and Small fail to disclose initiating an auto restore component.

For the same reasons as set forth above, Applicant's invention is not obvious in view of the cited references even when the further combination with the Pascucci reference is attempted. Reconsideration and a withdrawal of the rejection are hereby respectfully requested.

In addition, as Applicant previously pointed out in response to the previous office action, it would appear that one viewing Nachenberg (a reference relied on in the

rejection) would not have been led to employ an auto restore feature since Nachenberg desires to indicate whether or not a virus is present. The restoring would not be indicated as to what to restore to, since, according to Nachenberg, if a virus is not present, many changes could have occurred without a virus being present. Therefore, a restore point would first have to be indicated and Nachenberg would not be able to provide that option nor would it teach or suggest it. Accordingly, Applicant's invention is distinguishable, as pointed out above, and is further particularized in claims 12 and 24, in that the client state code provides the baseline and the hash code values represent a baseline so that clients on the network may be secured against intentional or unintentional file deletions or mishaps.

For the above reasons, and for these additional reasons, Applicant's invention, as recited in claims 12 and 24 should be patentable and the 103(a) rejection withdrawn.

Reconsideration and a withdrawal of the rejections is hereby respectfully requested.

CONCLUSION

Applicant's invention is not taught, suggested or disclosed by the cited references relied on by the Examiner. Accordingly, Applicant's presently claimed invention should be patentable.

If necessary, an appropriate extension of time to respond is respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required to Patent Office Deposit Account No. 05-0208.

Respectfully submitted,
JOHN F. A. EARLEY III
FRANK J. BONINI, JR.
CHARLES L. RIDDLE
HARDING, EARLEY, FOLLMER & FRAILEY
Attorneys for Applicant

Frank J. Bonini, Jr.
Registration No. 35,452
P.O. Box 750
Valley Forge, PA 19482-0750
Telephone: (610) 935-2300

Date: 7/17/08